

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

----- X
CISCO SYSTEMS, INC. and CISCO :
TECHNOLOGY, INC., :

Plaintiffs, :

-against- :

SHENZHEN TIANHENG NETWORKS CO; :
GEZHI PHOTONICS TECHNOLOGY CO., LTD.; :
SHENZHEN SOURCELIGHT TECHNOLOGY :
CO.; HU JIANGBING; LI PAN; DONG :
DAOSHUN; WANG WEI; and DARIOCOM, :

Defendants. :
----- X

19 Civ. _____

**DECLARATION OF
MICHAEL HEIDECKER**

**FILED *EX PARTE* AND UNDER SEAL
PURSUANT TO 15 U.S.C. § 1116**

Michael Heidecker, pursuant to 28 U.S.C. § 1746, hereby declares as follows:

1. I am familiar with the matters set forth in this declaration based upon my own personal knowledge. If called as a witness, I could and would competently testify to the following facts.

2. I submit this declaration in support of Plaintiffs' Order to Show Cause.

3. In particular, I make this declaration to explain my determination that the purported Cisco® brand pluggable transceiver modules ("Cisco transceivers") purchased by Marksmen Brand Protection Services ("Marksmen") from Defendants Shenzhen Tianheng Networks ("Shenzhen Tianheng"), Gezhi Photonics Technology Co., Ltd. ("Gezhi Photonics"), Shenzhen Sourcelight Technology Co. ("Shenzhen Sourcelight"), and Dariocom (collectively "Defendants") are counterfeit, and that these transceivers, including their sticker labels and electrically erasable programmable read-only ("EEPROM") memory, share characteristics that distinguish them from genuine Cisco transceivers.

4. There are numerous differences between authentic Cisco transceivers and the counterfeit transceivers purchased by Marksmen. However, in this declaration I will only disclose some of those differences so that I do not inadvertently provide a roadmap that enables Defendants (and other potential counterfeiters) to counterfeit Cisco products without detection.

Experience and Qualifications

5. I hold a Master of Information Systems and Bachelor of Science in Business Administration, both from University of Phoenix. I also attended California Polytechnic State University, San Luis Obispo, where I studied Electrical Engineering.

6. I began my professional career in 1985 as a product engineer for Hewlett Packard. During my fifteen years at Hewlett Packard, I became a manufacturing and product engineering manager. I was responsible for supervising product engineering teams, managing supplier product quality systems, customer audits and technical support, and conducting audits of product assembly. From 1999 through 2005, I worked at Agilent Technologies as a product engineering manager and R&D section manager, leading teams in new product development, intellectual property procurement, and post-release product quality. From 2005 to 2007, I worked as a product manager and product marketing engineer at Avago Technologies, where I managed certain transceiver module product market segments. And from 2007 to 2008, I worked for TekXs Consulting as a product authentication engineer, brand protection intelligence operation. At TekXs, I served as a consultant to Cisco Systems, Inc. ("Cisco"), coordinating, testing, and authenticating suspect counterfeit fiber optic transceiver products, and providing support to law enforcement authorities with authentication of Cisco products.

7. Since 2008, I have been employed by Cisco. During that time, I have served as a program manager and manager of operations in Cisco's Brand Protection Global Technical

Intelligence Operations. As program manager, I was initially responsible for the testing, analysis, and authentication of Cisco products in the United States and Canada. I subsequently became responsible for monitoring, inspecting, and reviewing Cisco's products, including transceivers, on a worldwide basis. In this role, my team and I work to ensure that all products that we review are genuine—that is, manufactured by Cisco or one of its authorized manufacturing partners—and not counterfeit products offered by third parties seeking to capitalize on Cisco's brand reputation for building reliable, high-quality products. I am also responsible for investigating customer complaints, as well as non-conformances, or deviations, in product that can occur during the manufacturing process. I am therefore very familiar with Cisco transceivers and their component parts, and the manner in which they are labeled and packaged for domestic and international sale.

Manufacturing, Labeling, and Monitoring of Genuine Cisco Transceivers

8. A transceiver is an electronic device that uses fiber optical technology to send (transmit) and receive data. A transceiver encodes and decodes data by converting an electrical signal into light pulses and then sends the data through a fiber optic cable, where it is received at the other end and converted back into an electrical signal. There are many models of Cisco transceivers which range in size, price, and functionality. Every Cisco transceiver, however, is designed to meet and exceed industry standards for quality, reliability, safety, and performance.

9. Cisco products are manufactured by, or often contain components that are manufactured by, third-party vendors called original equipment manufacturers ("OEMs"). Every OEM that Cisco utilizes is heavily vetted and scrutinized. The overwhelming majority of authentic Cisco transceivers are manufactured by one of three OEMs: FINISAR Corporation; Methode Electronics, Inc.; and Foxconn Interconnect Technology, Ltd ("FOIT"). These OEMs utilize

specialized equipment and heavily-tested processes to produce a consistent, high-performing product on which consumers rely.

10. Cisco places strict control requirements on its OEMs, each of whom must adhere to high quality manufacturing and distribution standards. These standards ensure that the product design meets feature specifications throughout the manufacturing lifecycle. Before a single product is shipped to a customer, Cisco conducts reliability demonstration testing to expose any undiscovered defects that may arise during the manufacturing process. After the product is approved for customer shipment, Cisco conducts ongoing reliability testing on subsequent productions. Cisco also ensures that each manufacturing facility meets its quality standards by subjecting each to stringent audits. Each OEM must maintain detailed production data records for each serialized product and must log product movement throughout the supply chain, which gives Cisco the ability to support customers via serial number traceability. In addition, each OEM participates in quarterly business reviews that comprehensively examine the manufacturer's practices and procedures and identify areas for improvement.

11. Each authentic transceiver that is manufactured by an authorized OEM is assigned a unique top label that is controlled by Cisco, printed by a security company under contract with Cisco, and sent directly to the OEM. The top label incorporates a multitude of overt and covert security features. In addition to having the Cisco brand name embossed on the label, the top label bears a product identification ("PID") number, a Cisco part number, a product label serial number, and a security label serial number. The product label serial number is a unique 11-digit alphanumeric figure with a 1-D barcode. The security label serial number is a unique 9-digit alphanumeric figure with a 2-D barcode. Importantly, all of these numbers must match up. If any

of these numbers do not match up—for instance, if the product label serial number is not associated with the proper PID and Cisco part numbers—then the product is a counterfeit.

12. Every Cisco transceiver also contains an EEPROM memory which stores a small amount of Cisco-specific data. The EEPROM content of an authentic Cisco transceiver identifies Cisco as the vendor, sets forth the product numbers identified above (including the Cisco part number and product label serial number), and includes a copyrighted and patented algorithm. This algorithm, which is referred to a “handshake,” is used to confirm that a valid Cisco transceiver has been deployed into the host device, for instance, a Cisco switch or Cisco router. The absence of any of this data on an EEPROM is evidence of a counterfeit, as is the presence of any incorrect information.

13. Cisco maintains three lab facilities dedicated to testing potentially counterfeit products around the world. The lab facilities are located in The Netherlands, Hong Kong, and San Jose, California—with this third facility being the largest. Generally, products are analyzed by the lab that is geographically closest to the procurement location. These test labs are access controlled—that is, only select members of the Cisco Brand Protection team are allowed to enter—to ensure that a proper chain of custody is maintained and that there is no tampering with products before, during, or after examination.

14. Cisco’s product authentication test labs are equipped with specialized tools to help Cisco’s Brand Protection engineers evaluate whether products are genuine, or whether they are counterfeit products bearing the Cisco trademark without authorization.

Receipt and Evaluation of Counterfeit Product


15. As part of our investigation into the counterfeit Cisco transceivers being offered by China-based entities online, I arranged for purchases from the Defendants by Marksmen. Unfortunately, the availability of counterfeit Cisco transceivers appears to be extensive.

16. For each purchase of a suspect Cisco transceiver from the Defendants, the product was delivered by the Defendant to an address in Brooklyn, New York. Under a stringent chain of custody, each suspect product was then shipped to Cisco's San Jose test lab. I then evaluated each product and determined (for the reasons set forth in the following paragraphs) that every one of these products was in fact counterfeit. To confirm my analysis, I took photographs of the suspect transceivers and shared these photos with the OEM, if any, that was identified in the counterfeit top label. Each OEM identified a set of potentially counterfeit attributes, which were evaluated by the OEM's test engineer. Based on this evaluation of every transceiver purchased from Defendants, the OEM's test engineer also determined that the suspect transceiver was counterfeit. I reviewed each OEM's findings, confirmed those findings, and adopted them as part of my comprehensive analysis of each counterfeit transceiver.

17. **Shenzhen Tianheng.** On July 15, 2019, Marksmen purchased six (6) transceivers from Shenzhen Tianheng at the following web address: <https://thnetwork.en.alibaba.com/>. Shenzhen Tianheng advertised and sold these transceivers as Cisco-brand transceivers. Shenzhen Tianheng sent these suspect transceivers to our investigators in Brooklyn, New York, who then sent the transceivers to Cisco's test lab in San Jose, California, for examination.

18. Specifically, Marksmen purchased the following transceivers from Shenzhen Tianheng using the following web addresses:

Model	Product ID	Product Label Serial Number	Security Label Serial Number	Web Address
GLC-SX-MMD	10-2626-01	FNS21040YHS	WA9MJ1795	https://thnetwork.en.alibaba.com/product/60556277631-219350195/CiscoSFPTTransceiver125G850nm550mGLCSXMMD.html
GLC-TE	30-1475-01	AVC19442363	W25NX4254	https://thnetwork.en.alibaba.com/product/60817810608-219350195/Cisco125GSFPTTransceiverGLCTE.html
SFP-10G-LR	10-2457-02	FNS19231A83	WAYG24492	https://thnetwork.en.alibaba.com/product/60817187936-219350195/Cisco_SFP_10G_Transceiver_SF_10G_LR_S.html
GLC-LH-SMD	10-2525-01	FNS17480SZB	A9JX2001	https://thnetwork.en.alibaba.com/product/60817053571-219350195/Cisco125GSFPTTransceiverGLCLHSMD.html
GLC-T	30-1410-03	AGM145121WC	W25LH3170	https://thnetwork.en.alibaba.com/product/60556863250-219350195/CiscoSFPTTransceiver125G1000BASETGLCT.html
SFP-10G-SR	10-2415-03	FNS1702214TN	WBN1H3867	https://thnetwork.en.alibaba.com/product/60531125534-219350195/CiscoSFP10GBASESRTransceiverSFP10GSR.html

19. On August 26, 2019, I examined all six suspect transceivers received from Shenzhen Tianheng. Each suspect transceiver had a top label that bore the Cisco logo: . Furthermore, the EEPROM for each transceiver identified “CISCO” as the vendor. I determined that each transceiver sold by Shenzhen Tianheng is not a genuine Cisco product, but instead is counterfeit.

20. I subsequently provided photographs of the suspect transceivers to the OEM identified in the product label serial number on the counterfeit top label: photographs of the products bearing the IDs 10-2626-01, 10-2457-02, 10-2525-01, and 10-2415-03 were provided to

FINISAR; and photographs of the products bearing the IDs 30-1475-01 and 30-1410-03 were provided to FOIT. The photographs of each product were reviewed and analyzed by the OEM's test engineer, who then prepared an ESR detailing his findings. FINISAR and FOIT confirmed my assessment, determining that all six suspect transceivers were counterfeit. I reviewed and adopted the OEMs' findings as part of my final assessment.

21. The suspect transceivers sold by Shenzhen Tianheng are clearly counterfeit in light of the many differences between them and authentic Cisco transceivers. These differences include, but are not limited to:


- (a) For genuine Cisco transceivers, the product label serial number and security label serial number are unique numbers that match up. The product label serial number and security label serial number on the Shenzhen Tianheng transceivers do not match.
- (b) Genuine Cisco transceivers are manufactured according to specific design and build standards, and use approved, genuine components. The counterfeit transceivers do not match Cisco's OEM build and design standards and use unapproved, non-genuine components.
- (c) The EEPROM of genuine Cisco transceivers identifies various product attributes, including the product part number, the vendor, the product serial label number, and a date code. The product attributes contained within the EEPROM for each counterfeit transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.

22. **Dariocom.** On July 15, 2019, Marksmen purchased two (2) transceivers from Amazon seller Dariocom. Dariocom advertised and sold these transceivers as Cisco-brand transceivers. Dariocom sent these suspect transceivers to our investigators in Brooklyn, New York, who sent them to Cisco's test lab in San Jose, California, for examination.

23. Specifically, Marksmen purchased the following transceivers from Dariocom using the following addresses:

Model	Product ID	Product Label Serial Number	Security Label Serial Number	Web Address
GLC-LH-SMD	10-2625-01	FNS17480SY3	WA9JV1999	https://www.amazon.com/gp/offer-listing/B00M8PLT14
GLC-T	30-1410-03	AGM145121VS	W25HS2643	https://www.amazon.com/gp/offer-listing/B0000C3GWT

24. On August 26, 2019, I examined the suspect transceivers received from Dariocom.

Each suspect transceiver had a top label that bore the Cisco logo: . Furthermore, the EEPROM for each transceiver identified “CISCO” as the vendor. I determined that each transceiver sold by Dariocom is not a genuine Cisco product, but instead is counterfeit.

25. I subsequently provided photographs of the transceivers received from Dariocom to the OEM identified in the product label serial number on the counterfeit top label: photographs of the product bearing the ID 10-2625-01 were provided to FINISAR; and photographs of the product bearing the ID 30-1410-03 were provided to FOIT. The photographs of each product were reviewed and analyzed by the OEM’s test engineer, who then prepared an ESR detailing his findings. FINISAR and FOIT confirmed my assessment, determining that the two Dariocom transceivers were counterfeit. I reviewed and adopted the OEMs’ findings as part of my final assessment.

26. The suspect transceivers sold by Dariocom are clearly counterfeit in light of the many differences between them and authentic Cisco transceivers. These differences include, but are not limited to:

- (a) For genuine Cisco transceivers, the product label serial number and security label serial number are unique numbers that match up. The product label serial number and security label serial number on the Dariocom transceivers do not match.

- (b) Genuine Cisco transceivers are manufactured according to specific design and build standards, and use approved, genuine components. The counterfeit transceivers do not match Cisco's OEM build and design standards and use unapproved, non-genuine components.
- (c) The EEPROM of genuine Cisco transceivers identifies various product attributes, including the product part number, the vendor, the product serial label number, and a date code. The product attributes contained within the EEPROM for each counterfeit transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.

27. **Gezhi Photonics.** On August 23, 2019, Marksmen purchased two (2) transceivers from Gezhi Photonics at the following web address: <https://gezhiphotonics.en.alibaba.com/>. Gezhi Photonics advertised and sold these transceivers as Cisco-brand transceivers. Gezhi Photonics sent these suspect transceivers to our investigators in Brooklyn, New York, who sent them to Cisco's test lab in San Jose, California, for examination.

28. Specifically, Marksmen purchased the following transceivers from Gezhi Photonics using the following web addresses:

Model	Product ID	Product Label Serial Number	Security Label Serial Number	Web Address
SFP-10G-LR-X	N/A	GS1909090001	N/A	https://gezhiphotonics.en.alibaba.com/product/60419472585-806982708/CiscoSFP101001000baseTCopperTransceiverGLCT.html
SFP-10G-LR-X	N/A	GS1909090002	N/A	https://gezhiphotonics.en.alibaba.com/product/60419472585-806982708/CiscoSFP101001000baseTCopperTransceiverGLCT.html

29. On September 30, 2019, I examined the suspect transceivers received from Gezhi Photonics. The EEPROM for each transceiver identified "CISCO" as the vendor. I determined that each transceiver sold by Gezhi Photonics is not a genuine Cisco product, but instead is counterfeit.

30. The top label of the suspect transceivers sold by Gezhi Photonics did not indicate an OEM. Accordingly, I did not provide photographs of the suspect transceivers to an OEM. Therefore, my preliminary assessment and final assessment are one and the same. Because authentic product always contains a top label that indicates an OEM, the lack of such information on the top label of the transceivers sold by Gezhi Photonics is itself evidence that the product is counterfeit.

31. The suspect transceivers sold by Gezhi Photonics are clearly counterfeit in light of the many difference between them and authentic Cisco transceivers. These differences include, but are not limited to:

- (a) The top label of each Gezhi Photnoics transceiver is not consistent with authentic Cisco transceiver top labels. The product label serial number on each Gezhi Photonics transceiver does not meet the Cisco-approved product label serial number format or nomenclature.
- (b) The attributes contained within the EEPROM for each Gezhi Photonics transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.

32. The counterfeit transceivers sold by Gezhi Photonics are programmed to deceive the consumer into thinking they are genuine Cisco transceivers. For example, the EEPROM for each Gezhi Photonics transceiver contains the Cisco copyrighted and patented “handshake” algorithm in order to emulate a genuine Cisco transceiver (and thereby deceive the end user) when connected to a Cisco host device.

33. **Shenzhen Sourcelight.** On September 11, 2019, Marksmen purchased two (2) transceivers from Shenzhen Sourcelight at the following web address: <https://sourcelighten.en.alibaba.com/>. Shenzhen Sourcelight advertised and sold these transceivers as Cisco-brand transceivers. Shenzhen Sourcelight sent these suspect transceivers to

our investigators in Brooklyn, New York, who sent them to Cisco's test lab in San Jose, California, for examination.

34. Specifically, Marksmen purchased the following transceivers from Shenzhen Sourcelight using the following web addresses:

Model	Product ID	Product Label Serial Number	Security Label Serial Number	Web Address
SFP-10G-LR	N/A	1SLU1909110001	N/A	https://sourcelightcn.en.alibaba.com/product/60643189026-806494291/Cisco_SFP_10G_LR_X_for_10GBASE_LR_1310nm_10Km_DDM_extended_temperature_range.html
SFP-10G-LR	N/A	1SLU1909110002	N/A	https://sourcelightcn.en.alibaba.com/product/60643189026-806494291/Cisco_SFP_10G_LR_X_for_10GBASE_LR_1310nm_10Km_DDM_extended_temperature_range.html

35. On September 30, 2019, I examined the suspect transceivers received from Shenzhen Sourcelight. The EEPROM for each transceiver identified "CISCO" as the vendor. I determined that each transceiver sold by Shenzhen Sourcelight is not a genuine Cisco product, but instead is counterfeit.

36. The top label of the suspect transceivers sold by Shenzhen Sourcelight did not indicate an OEM. Accordingly, I did not provide photographs of the suspect transceivers to an OEM. Therefore, my preliminary assessment and final assessment are one and the same. Because authentic product always contains a top label indicating an OEM, the lack of such information on the top label of the transceivers sold by Gezhi Photonics is itself evidence that the product is counterfeit.

37. The suspect transceivers sold by Shenzhen Sourcelight are clearly counterfeit in light of the many difference between them and authentic Cisco transceivers. These differences include, but are not limited to:

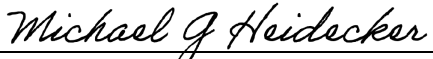
- (a) The top label of each Shenzhen Sourcelight transceiver is not consistent with authentic Cisco transceiver top labels. The product label serial number on each Shenzhen Sourcelight transceiver does not meet the Cisco-approved product label serial number format or nomenclature.
- (b) The attributes contained within the EEPROM for each Shenzhen Sourcelight transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.

38. Like those sold by Gezhi Photonics, the suspect transceivers sold by Shenzhen Sourcelight are programmed to deceive the consumer into thinking that they are genuine Cisco transceivers. The EEPROM for each suspect transceiver contains the Cisco copyrighted and patented “handshake” algorithm attributes in order to emulate a genuine Cisco transceiver (and deceive the end user).

39. In summary, all of the products listed above and purchased from Defendants share various distinctive characteristics that distinguish them from genuine products manufactured by or for Cisco. Those distinctive characteristics do not and could not appear on authentic Cisco transceivers. It is therefore my firm conclusion that all of the suspect transceivers sold by the Defendants are counterfeit.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on November 18, 2019



Michael Heidecker